

AMENDMENTS TO THE CLAIMS

Please cancel Claims 10, 22, 33, and 45.

Please amend Claims 1-5, 7-9, 11-17, 19-21, 23-28, 30-32, 34-40, 42-44, and 46 as follows:

- 1 1. (Currently amended) A process for storing and recovering security information
- 2 stored on a first transportable memory device ~~smart-card~~ that is used to uniquely access a
- 3 client computer and secure logins into networks and Web sites, comprising the steps of:
- 4 providing a secure server;
- 5 creating a password and challenge question;
- 6 wherein said password is used to access said server if said first transportable
- 7 memory device ~~smart-card~~ is lost and said challenge question is used to confirm the user's
- 8 identity when challenged while accessing said server without a transportable memory device
- 9 ~~smart-card~~;
- 10 retrieving ~~the~~ an ID number of said first transportable memory device ~~smart-card~~ and
- 11 other user and system specific information;
- 12 storing said first transportable memory device ~~smart-card~~ ID and said other user and
- 13 system specific information on said server;
- 14 providing access key creation means on said server for creating a first access key;
- 15 storing said first access key on said server; ~~and~~
- 16 providing configuration means for configuring said client to boot only if said first
- 17 transportable memory device ~~smart-card~~ is readable by said client or said first access key is
- 18 entered[.];
- 19 wherein said access key creation means creates a second access key upon request by
- 20 the user;

21 replacing said first access key with said second access key on said server; and
 22 wherein said configuration means configures said client to boot if said second access
 23 key is entered, thereby replacing said first access key.

1 2. (Currently amended) The process of claim 1, wherein an emergency diskette is
 2 created and said client can boot using said diskette instead of said first transportable
 3 memory device smart-card.

1 3. (Currently amended) The process of claim 1, wherein the user accesses said server
 2 through another computer; wherein said server requires the user to log in; and wherein said
 3 server displays ~~said~~ a current access key to the user if said log in is correct.

1 4. (Currently amended) The process of claim 1, wherein the user enters ~~said first a~~
 2 current access key into said client; and wherein said client boots in response to ~~said first~~
 3 current access key.

1 5. (Currently amended) The process of claim 1, further comprising the steps of:
 2 wherein the user requests that said server issue a second transportable memory
 3 device smart-card to replace said first transportable memory device smart-card;
 4 ~~wherein the user makes said request through said client;~~
 5 retrieving the ID number from said second transportable memory device smart-card;
 6 replacing said first transportable memory device smart-card's ID with said second
 7 transportable memory device smart-card's ID on said server; and

8 wherein said configuration means configures said client to boot if said second
 9 transportable memory device ~~smart-card~~ is readable, thereby replacing said first
 10 transportable memory device ~~smart-card~~.

1 6. (Original) The process of claim 5, wherein said server requires the user to enter the
 2 proper user and/or other system specific information to validate said request.

1 7. (Currently amended) The process of claim 5, further comprising the step of:
 2 wherein said access key creation means creates a ~~second~~ third access key;
 3 replacing said first access key with said ~~second~~ third access key on said server; and
 4 wherein said configuration means configures said client to boot if said ~~second~~ third
 5 access key is entered, thereby replacing said first access key.

1 8. (Currently amended) The process of claim 5, further comprising the step of:
 2 providing morphing means for recreating ~~the~~ a personal computing environment
 3 stored on said first transportable memory device ~~smart-card~~ onto said second transportable
 4 memory device ~~smart-card~~.

1 9. (Currently amended) The process of claim 8, wherein said morphing means
 2 transfers ~~the~~ encryption and other rights of said first transportable memory device ~~smart~~
 3 ~~card~~ to said second transportable memory device ~~smart-card~~.

1 10. (Canceled)

1 11. (Currently amended) The process of claim 1, further comprising the step of:
2 providing automatic login means resident on said client for logging onto networks
3 and/or Web sites, without the user's intervention, using the user's information stored on said
4 first transportable memory device ~~smart card~~.

1 12. (Currently amended) A process for storing and recovering security information
2 stored on a first transportable memory device ~~smart card~~ that is used to uniquely access a
3 client computer, comprising the steps of:
4 providing a secure server;
5 retrieving the ID number of said first transportable memory device ~~smart card~~ and
6 other user and system specific information;
7 storing said first smart card ID and said other user and system specific information
8 on said server;
9 providing access key creation means on said server for creating a first access key;
10 storing said first access key on said server; ~~and~~
11 providing configuration means for configuring said client to boot only if said first
12 transportable memory device ~~smart card~~ is readable by said client or said first access key is
13 entered[.];
14 wherein said access key creation means creates a second access key upon request by
15 the user;
16 replacing said first access key with said second access key on said server; and
17 wherein said configuration means configures said client to boot if said second access
18 key is entered, thereby replacing said first access key.

1 13. (Currently amended) The process of claim 12, further comprising the step of:
2 creating a password and challenge question; and
3 wherein said password is used to access said server if said first transportable
4 memory device ~~smart-card~~ is lost and said challenge question is used to confirm the user's
5 identity when challenged while accessing said server without a transportable memory device
6 ~~smart-card~~.

1 14. (Currently amended) The process of claim 12, wherein an emergency diskette is
2 created and said client can boot using said diskette instead of said first transportable
3 memory device ~~smart-card~~.

1 15. (Currently amended) The process of claim 13, wherein the user accesses said server
2 through another computer; wherein said server requires the user to log in; and wherein said
3 server displays ~~said~~ a current access key to the user if said log in is correct.

1 16. (Currently amended) The process of claim 12, wherein the user enters ~~said-first~~ a
2 current access key into said client; and wherein said client boots in response to said ~~first~~
3 current access key.

1 17. (Currently amended) The process of claim 12, further comprising the steps of:
2 wherein the user requests that said server issue a second transportable memory
3 device ~~smart-card~~ to replace said first transportable memory device ~~smart-card~~;
4 ~~wherein the user makes said request through said client;~~
5 retrieving the ID number from said second transportable memory device ~~smart-card~~;

6 replacing said first transportable memory device ~~smart-card~~'s ID with said second
 7 transportable memory device ~~smart-card~~'s ID on said server; and
 8 wherein said configuration means configures said client to boot if said second
 9 transportable memory device ~~smart-card~~ is readable, thereby replacing said first
 10 transportable memory device ~~smart-card~~.

1 18. (Original) The process of claim 17, wherein said server requires the user to enter the
 2 proper user and/or other system specific information to validate said request.

1 19. (Currently amended) The process of claim 17, further comprising the step of:
 2 wherein said access key creation means creates a ~~second~~ third access key;
 3 replacing said first access key with said ~~second~~ third access key on said server; and
 4 wherein said configuration means configures said client to boot if said ~~second~~ third
 5 access key is entered, thereby replacing said first access key.

1 20. (Currently amended) The process of claim 17, further comprising the step of:
 2 providing morphing means for recreating ~~the~~ a personal computing environment
 3 stored on said first transportable memory device ~~smart-card~~ onto said second transportable
 4 memory device ~~smart-card~~.

1 21. (Currently amended) The process of claim 20, wherein said morphing means
 2 transfers ~~the~~ encryption and other rights of said first transportable memory device ~~smart~~
 3 ~~card~~ to said second transportable memory device ~~smart-card~~.

1 22. (Canceled)

1 23. (Currently amended) The process of claim 12, further comprising the step of:
2 providing automatic login means on said client for logging onto networks and/or
3 Web sites, without the user's intervention, using the user's information stored on said first
4 transportable memory device ~~smart-card~~.

1 24. (Currently amended) A program storage medium readable by a computer, tangibly
2 embodying a program of instructions executable by the computer to perform method steps
3 for storing and recovering security information stored on a first transportable memory
4 device ~~smart-card~~ that is used to uniquely access a client computer, comprising the steps of:
5 providing a secure server;
6 creating a password and challenge question;
7 wherein said password is used to access said server if said first transportable
8 memory device ~~smart-card~~ is lost and said challenge question is used to confirm the user's
9 identity when challenged while accessing said server without a transportable memory device
10 ~~smart-card~~;
11 retrieving the ID number of said first transportable memory device ~~smart-card~~ and
12 other user and system specific information;
13 storing said first transportable memory device ~~smart-card~~ ID and said other user and
14 system specific information on said server;
15 providing access key creation means on said server for creating a first access key;
16 storing said first access key on said server; and

17 providing configuration means for configuring said client to boot only if said first
 18 transportable memory device ~~smart-card~~ is readable by said client or said first access key is
 19 entered[[.]] ;

20 wherein said access key creation means creates a second access key upon request by
 21 the user;

22 replacing said first access key with said second access key on said server; and

23 wherein said configuration means configures said client to boot if said second access
 24 key is entered, thereby replacing said first access key.

1 25. (Currently amended) The method of claim 24, wherein an emergency diskette is
 2 created and said client can boot using said diskette instead of said first transportable
 3 memory device ~~smart-card~~.

1 26. (Currently amended) The method of claim 24, wherein the user accesses said server
 2 through another computer; wherein said server requires the user to log in; and wherein said
 3 server displays said a current access key to the user if said log in is correct.

1 27. (Currently amended) The method of claim 24, wherein the user enters ~~said first a~~
 2 ~~current~~ access key into said client; and wherein said client boots in response to said ~~first~~
 3 current access key.

1 28. (Currently amended) The method of claim 24, further comprising the steps of:
 2 wherein the user requests that said server issue a second transportable memory
 3 device ~~smart-card~~ to replace said first transportable memory device ~~smart-card~~;

4 ~~wherein the user makes said request through said client;~~
 5 retrieving the ID number from said second transportable memory device ~~smart card~~;
 6 replacing said first transportable memory device ~~smart card~~'s ID with said second
 7 transportable memory device ~~smart card~~'s ID on said server; and
 8 wherein said configuration means configures said client to boot if said second
 9 transportable memory device ~~smart card~~ is readable, thereby replacing said first
 10 transportable memory device ~~smart card~~.

1 29. (Original) The method of claim 28, wherein said server requires the user to enter the
 2 proper user and/or other system specific information to validate said request.

1 30. (Currently amended) The method of claim 28, further comprising the step of:
 2 wherein said access key creation means creates a ~~second~~ third access key;
 3 replacing said first access key with said ~~second~~ third access key on said server; and
 4 wherein said configuration means configures said client to boot if said ~~second~~ third
 5 access key is entered, thereby replacing said first access key.

1 31. (Currently amended) The method of claim 28, further comprising the step of:
 2 providing morphing means for recreating ~~the~~ a personal computing environment
 3 stored on said first transportable memory device ~~smart card~~ onto said second transportable
 4 memory device ~~smart card~~.

1 32. (Currently amended) The method of claim 31, wherein said morphing means
2 transfers the encryption and other rights of said first transportable memory device ~~smart~~
3 ~~card~~ to said second transportable memory device ~~smart card~~.

1 33. (Canceled)

1 34. (Currently amended) The method of claim 24, further comprising the step of:
2 providing automatic login means resident on said client for logging onto networks
3 and/or Web sites, without the user's intervention, using the user's information stored on said
4 first transportable memory device ~~smart card~~.

1 35. (Currently amended) A program storage medium readable by a computer, tangibly
2 embodying a program of instructions executable by the computer to perform method steps
3 for storing and recovering security information stored on a first transportable memory
4 device ~~smart card~~ that is used to uniquely access a client computer, comprising the steps of:
5 providing a secure server;
6 retrieving the ID number of said first transportable memory device ~~smart card~~ and
7 other user and system specific information;
8 storing said first transportable memory device ~~smart card~~ ID and said other user and
9 system specific information on said server;
10 providing access key creation means on said server for creating a first access key;
11 storing said first access key on said server; and

12 providing configuration means for configuring said client to boot only if said first
 13 transportable memory device ~~smart-card~~ is readable by said client or said first access key is
 14 entered[[]] ;
 15 wherein said access key creation means creates a second access key upon request by
 16 the user;
 17 replacing said first access key with said second access key on said server; and
 18 wherein said configuration means configures said client to boot if said second access
 19 key is entered, thereby replacing said first access key.

1 36. (Currently amended) The method of claim 35, further comprising the step of:
 2 creating a password and challenge question; and
 3 wherein said password is used to access said server if said first transportable
 4 memory device ~~smart-card~~ is lost and said challenge question is used to confirm the user's
 5 identity when challenged while accessing said server without a transportable memory device
 6 ~~smart-card~~.

1 37. (Currently amended) The method of claim 35, wherein an emergency diskette is
 2 created and said client can boot using said diskette instead of said first transportable
 3 memory device ~~smart-card~~.

1 38. (Currently amended) The method of claim 36, wherein the user accesses said server
 2 through another computer; wherein said server requires the user to log in; and wherein said
 3 server displays said a current access key to the user if said log in is correct.

1 39. (Currently amended) The method of claim 35, wherein the user enters ~~said first a~~
2 current access key into said client; and wherein said client boots in response to said ~~first~~
3 current access key.

1 40. (Currently amended) The method of claim 35, further comprising the steps of:
2 wherein the user requests that said server issue a second transportable memory
3 device smart-card to replace said first transportable memory device smart-card;
4 ~~wherein the user makes said request through said client;~~
5 retrieving the ID number from said second transportable memory device smart-card;
6 replacing said first transportable memory device smart-card's ID with said second
7 transportable memory device smart-card's ID on said server; and
8 wherein said configuration means configures said client to boot if said second
9 transportable memory device smart-card is readable, thereby replacing said first
10 transportable memory device smart-card.

11

1 41. (Original) The method of claim 40, wherein said server requires the user to enter the
2 proper user and/or other system specific information to validate said request.

1 42. (Currently amended) The method of claim 40, further comprising the step of:
2 wherein said access key creation means creates a ~~second~~ third access key;
3 replacing said first access key with said ~~second~~ third access key on said server; and
4 wherein said configuration means configures said client to boot if said ~~second~~ third
5 access key is entered, thereby replacing said first access key.

1 43. (Currently amended) The method of claim 40, further comprising the step of:
2 providing morphing means for recreating ~~the~~ a personal computing environment
3 stored on said first transportable memory device ~~smart-card~~ onto said second transportable
4 memory device ~~smart-card~~.

1 44. (Currently amended) The method of claim 43, wherein said morphing means
2 transfers ~~the~~ encryption and other rights of said first transportable memory device ~~smart~~
3 ~~card~~ to said second transportable memory device ~~smart-card~~.

1 45. (Canceled)

1 46. (Currently amended) The method of claim 35, further comprising the step of:
2 providing automatic login means resident on said client for logging onto networks
3 and/or Web sites, without the user's intervention, using the user's information stored on said
4 first transportable memory device ~~smart-card~~.